524 Rec'd PCT/PTO 01 OCT 1999

FORM PTO-1390 (REV. 5-93) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTORNEY'S DOCKET NUMBER **2345/91**
TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371	U.S. APPLICATION NO. (If known, see 37 CFR 1.5) 09/402322

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED:
PCT/EP98/08057	10 December 1998 (10.12.98)	02 February 1998 (02.02.98)

TITLE OF INVENTION
METHOD AND ARRANGEMENTS FOR GENERATING BINARY SEQUENCES OF RANDOM NUMBERS

APPLICANT(S) FOR DO/EO/US
DULTZ, Wolfgang; DULTZ, Gisela; HILDEBRANDT, Eric; and SCHMITZER, Heidrun

Applicant(s) herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) immediately rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☐ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☒ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US)
6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)). Unsigned
10 ☒ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern other document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A **FIRST** preliminary amendment.
    ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
14. ☐ A substitute specification.
15. ☐ A change of power of attorney and/or address letter.
16. ☒ Other items or information: International Search Report.

Express Mail No.: EL179668825US

U.S. APPLICATION NO. if known, see 37 C.F.R 1.5 09/402322	INTERNATIONAL APPLICATION NO. PCT/EP98/08057	ATTORNEY'S DOCKET NUMBER 2345/91

430 Rec'd PCT/PTO 01 OCT 1999

17. ☒ The following fees are submitted:

	CALCULATIONS	PTO USE ONLY
Basic National Fee (37 CFR 1.492(a)(1)-(5)): Search Report has been prepared by the EPO or JPO .... $840.00 International preliminary examination fee paid to USPTO (37 CFR 1.482) ... $670.00 No international preliminary examination fee paid to USPTO (37 CFR 1.482) but international search fee paid to USPTO (37 CFR 1.445(a)(2)) .... $760.00 Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO .... $970.00 International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4) $96.00		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 840	
Surcharge of $130.00 for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$	

Claims	Number Filed	Number Extra	Rate		
Total Claims	11 - 20 =	0	X $18.00	$0	
Independent Claims	2 - 3 =	0	X $78.00	$0	
Multiple dependent claim(s) (if applicable)			+ $260.00	$0	
TOTAL OF ABOVE CALCULATIONS =				$840	
Reduction by 1/2 for filing by small entity, if applicable. Verified Small Entity statement must also be filed. (Note 37 CFR 1.9, 1.27, 1.28).				$	
SUBTOTAL =				$840	
Processing fee of $130.00 for furnishing the English translation later the ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(f)). +				$	
TOTAL NATIONAL FEE =				$840	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). $40.00 per property +				$	
TOTAL FEES ENCLOSED =				$840	
				Amount to be: refunded	$
				charged	$

a. ☐ A check in the amount of $__________ to cover the above fees is enclosed.

b. ☒ Please charge my Deposit Account No. 11-0600 in the amount of $840.00 to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 11-0600. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Kenyon & Kenyon
One Broadway
New York, New York 10004

SIGNATURE

Richard L. Mayer, Reg. No. 22,490
NAME

10/1/99
DATE

223507

09/402322
430 Rec'd PCT/PTO 01 OCT 1999

[2345/91]

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT: DULTZ ET AL.

SERIAL NO.: to be assigned

FILED: herewith

TITLE: METHOD AND ARRANGEMENT FOR GENERATING BINARY SEQUENCES OF RANDOM NUMBERS

ART UNIT: not yet known

EXAMINER: not yet known

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

PRELIMINARY AMENDMENT

Please amend the above-identified application before a first consideration on the merits as follows:

IN THE SPECIFICATION

On page 1, line 1, change "Description" to --Field of the Invention--.

On page 1, line 3, after "arrangement" insert --and method--.

On page 1, before line 6, insert --Related Technology--.

On page 3, line 9, after "1994" insert --, which is hereby incorporated by reference herein--.

On page 3, before line 13, insert --Summary of the Invention--.

On page 3, line 13, change Tthe object" to --An object--.

On page 3, line 15, change "above. This method should be" to --above, while being-- and change "the known methods and should be" to --prior methods and--.

On page 3, delete lines 18-20.

On page 3, before line 22, insert --The present invention provides a method of generating a binary sequence of random numbers based on random selection of a path of

2L179668825US

photons on a beam splitter, the method including emitting photons or photon swarms according to a randomness principle using a photon source, the photon source including a low power light source; splitting the photons or photon swarms emitted by the photon source during a measurement period using at least a first beam splitter and a second beam splitter disposed in a beam path of the light source, the second beam splitter being disposed downstream of the first beam splitter in a first downstream path of the first beam splitter; detecting, in accordance with the splitting, the photons or photon swarms from the splitting using a first, a second and a third detector connected to a detection device, the first detector being disposed in a second downstream path of the first beam splitter, the second detector being disposed in a third downstream path of the second beam splitter, the third detector being disposed in a fourth downstream path of the second beam splitter; generating a random number when the photons or photon swarms detected at the first, second and third detectors together correspond to a predefined photon scheme, the photon scheme including generating a random number when only one of the second and third detectors registers a detection of the photons or photon swarms.

The present invention also provides an apparatus for generating a binary sequence of random numbers, the apparatus including a low power light source including a photon source for emitting individual photons and/or photon swarms according to a randomness principle; a first and a second beam splitter disposed downstream from the light source in a beam path of the light source, the first beam splitter being disposed between the light source and the second beam splitter; a first detector disposed in a downstream path of the first beam splitter; a second detector and a third detector disposed in a first and a second downstream path, respectively, of the second beam splitter; a detection device for generating the random numbers, the detection device being disposed downstream from the first, second and third detectors, the detection device including at least one counter and computer.--.

On page 3, line 22, change "is based on" to --uses--.

On page 4, line 17, change "The mathematical principles and the possible embodiments" to --Embodiments--.

On page 4, before line 17, insert--<u>Brief Description of the Drawings</u>--.

On page 4, delete line 17.

On page 4, line 18, change "to the present invention are" to --The present invention is-- and change "Figure" to --the drawing,--.

On page 4, line 19, change "1." to --in which:

Figure 1 shows a schematic representation of an arrangement for generating binary sequences.--

On page 4, before line 21, insert --Detailed Description--.

On page 4, line 21, change "Light" to --Referring to Figure 1, light--.

On page 6, line 16, change "used here" to --according to the present invention--.

One page 7, line 12, change "is" to --are--.

On page 8, line 8, change "$D1_0$ I" to --$D1_0$, $D2_1$ detectors of the second beam splitter--.

On page 8, delete lines 9-10.

On page 9, line 1, change "Patent Claims" to --WHAT IS CLAIMED IS:--.

IN THE CLAIMS

Please cancel claims 1-10 and add new claims 11-21 as follows:

--11. (new) A method of generating a binary sequence of random numbers based on random selection of a path of photons on a beam splitter, the method comprising:

emitting photons or photon swarms according to a randomness principle using a photon source, the photon source including a low power light source;

splitting the photons or photon swarms emitted by the photon source during a measurement period using at least a first beam splitter and a second beam splitter disposed in a beam path of the light source, the second beam splitter being disposed downstream of the first beam splitter in a first downstream path of the first beam splitter;

detecting, in accordance with the splitting, the photons or photon swarms from the splitting using a first, a second and a third detector connected to a detection device, the first detector being disposed in a second downstream path of the first beam splitter, the second detector being disposed in a third downstream path of the second beam splitter, the third detector being disposed in a fourth downstream path of the second beam splitter;

generating a random number when the photons or photon swarms detected at the first, second and third detectors together correspond to a predefined photon scheme, the photon scheme including generating a random number when only one of the second and third detectors registers a detection of the photons or photon swarms.

12. (new) The method as recited in claim 11 wherein the photon scheme includes generating a random number when during the measurement period no photon of the photons or photon swarms is detected at the first detector and at least one photon of the photons or photon swarms is detected at only one of the second and third detectors.

13. (new) The method as recited in claim 11 wherein the photon scheme includes generating a random number when during the measurement period at least one photon of the photons or photon swarms is detected at the first detector and at least one photon of the photons or photon swarms is detected at only one of the second and third detectors.

14. (new) The method as recited in claim 11 wherein the at least a first and second beam splitters includes at least a third beam splitter disposed in the beam path between the light source and the second beam splitter, each of the at least a third beam splitter including an associated fourth detector disposed in a respective downstream path of the associated at least a third beam splitter, the photon scheme including generating a random number only when a photon swarm of the photons or photon swarms including a number of photons defined by the photon scheme is detected at the first, second, third and fourth detectors.

15. (new) An apparatus for generating a binary sequence of random numbers, the apparatus comprising:

a low power light source including a photon source for emitting individual photons and/or photon swarms according to a randomness principle;

a first and a second beam splitter disposed downstream from the light source in a beam path of the light source, the first beam splitter being disposed between the light source and the second beam splitter;

a first detector disposed in a downstream path of the first beam splitter;

a second detector and a third detector disposed in a first and a second downstream path, respectively, of the second beam splitter;

a detection device for generating the random numbers, the detection device being disposed downstream from the first, second and third detectors, the detection device including at least one counter and computer.

16. (new) The apparatus as recited in claim 15 wherein the first beam splitter includes a trigger beam splitter and the first detector includes a trigger detector .

17. (new) The apparatus as recited in claim 15 wherein the photon source includes an attenuated laser.

18. (new) The apparatus as recited in claim 15 wherein the photon source includes a thermal light source.

19. (new) The apparatus as recited in claim 15 wherein the photon source includes a spectral lamp.

20. (new) The apparatus as recited in claim 15 wherein the photon source includes a light emitting diode.

21. (new) The apparatus as recited in claim 15 wherein the photon source includes a pinched light source.--

<u>IN THE ABSTRACT</u>

Line 1, change "1.1. Method" to --A method--.

Delete lines 2-6.

Line 7, change "2.2. This method is based on" to --uses--.

Delete lines 16-19.

REMARKS

This Preliminary Amendment cancels original claims 1-10 in the underlying PCT Application No. PCT/EP98/08057, and adds new claims 11-21. The new claims do not add new matter to the application but do conform the claims to U.S. Patent and Trademark Office rules.

The amendments to the specification and abstract are to conform the specification and abstract to U.S. Patent and Trademark Office rules and do not introduce new matter into the application.

The underlying PCT application includes an International Search Report (copy included).

Conclusion

Consideration of the present application as amended is hereby respectfully requested.

Respectfully Submitted,

Kenyon & Kenyon

Dated: 8 September 1999

By: Erik R. Swanson

Erik R. Swanson
(Reg. No. 40,833)

One Broadway
New York, NY 10004
(212) 425-7200

//PRTS

09/402322

430 Rec'd PCT/PTO 01 OCT 1999

[2345/91]

METHOD AND ARRANGEMENT FOR GENERATING BINARY SEQUENCES OF RANDOM NUMBERS

Description

The present invention relates to an arrangement for generating binary sequences of random numbers.

Random numbers are used in mathematical simulation of random processes, in random sampling and in cryptology in particular. Due to increasing high-bit-rate digital communications over publically accessible communication channels, guaranteeing the confidentiality and authenticity of the information transmitted has become a central problem. Good cryptographic codes are sequences of random binary numbers. For secure encoding, preferably a random code of this type is selected; this code is as long as the message itself and is used only once.

Essentially two different options are available for generating random numbers:

1. Pseudo-random numbers generated by mathematical algorithms
Essentially, true random numbers cannot be generated by a computer, which operates completely deterministically. Therefore, the random numbers generated by mathematical algorithms and provided by many programs are never truly random. Pseudo-random numbers, developed from a shorter, truly random nucleus are an improvement.

In any case, however, a certain number of sequences that are not usable from the beginning (weak keys) must be expected in generating pseudo-random numbers by the methods described above, and in any case, odd correlations must be expected.

2. Random numbers based on physical methods

ZL179668825US

These methods make use of the random character of certain physical processes.

Even with the physical methods, there are those which are fundamentally deterministic, but are so complex that they cannot be reproduced. This would include, for example, a coin throw of heads or tails or lotto machines. These methods generate a deterministic chaos, which may be considered random because the initial conditions of the generator in generating each individual random number are always slightly different each time, without this difference being quantifiable. The physical methods also include elementary processes, such as those in quantum mechanics. Such processes are naturally basically random. Random numbers generated by physical processes therefore come closer to the concept of a random sequence than do random numbers generated by an algorithm.

There is a known solution utilizing the natural quantum process of the electromagnetic noise of a resistor or a diode to generate random bit sequences (see Manfred Richter: "Ein Rauschgenerator zur Gewinnung von quasiidealen Zufallszahlen für die stochastische Simulation" [A noise generator for generating quasi-ideal random numbers for stochastic simulation], Dissertation RWTH Aachen; 1992).

However, such methods can be manipulated externally by superimposing an arbitrary predetermined "noise" on the quantum noise, e.g., from incident electromagnetic waves. Since it is not easy to separate quantum noise from such an externally imposed pseudo-noise, these methods are not considered to be secure.

In addition, there are known methods of generating random numbers based on radioactive decay processes (see Martin Gude: "Ein quasi-idealer Gleichverteilungsgenerator basierend auf physikalischen Zufallsphänomenen" [A quasi-ideal uniform distribution generator based on physical random phenomena], Dissertation, RWTH Aachen 1987). This method is very suitable for generating random sequences because of the high energy of the resulting particles, but in addition

to the very real risks, due in particular to the potentially harmful effect of radioactive radiation on humans, there is also an irrational prejudice against radioactivity on the part of some of the population, so that radioactive processes cannot readily be used for random generation.

Another known method of generating random sequences is based on the process of selecting the path of individual photons on a beam splitter (see J. G. Rarity et al.: "Quantum random-number generation and key sharing" J. Mod. Opt. 41, p. 2435, 1994). In this method, a light quantum is reflected or transmitted on a semitransparent mirror, for example; two detectors record the light quantum and their displays represent the "0" or "1" of the random sequence.

The object of the present invention is to provide a method and an arrangement for generating binary sequences of random numbers to avoid the disadvantages described above. This method should be less expensive than the known methods and should be suitable for integration onto a chip card without any great complexity.

This object is achieved according to the present invention by the characterizing features of Patent Claim 1. Advantageous embodiments and refinements are derived from the subclaims.

The method according to the present invention is based on the known principle of selecting the path of individual photons on a beam splitter. With the method according to the present invention, ultraviolet, visible or infrared light strikes an optical beam splitter, e.g., a semitransparent mirror. Two detectors which can detect individual photons register the photons and define the "0" or the "1" of the random sequence via the displays assigned to them and thus define the random sequence itself.

With the method according to the present invention, a photon source of a low power and thus also small dimension is used as light source L instead of the photon source

customary in the past, such as an attenuated laser beam source. For example, attenuated laser diodes, normal diodes (LEDs), thermal light sources such as halogen lamps, spectral lamps or pinched light sources are suitable. In addition, according to the present invention, a first beam splitter ST1, preferably a trigger beam splitter, is inserted into the beam path of light source L upstream from second beam splitter ST2. The photons/photon swarms emitted during a predefined measurement time by light source L according to the random principle are split by beam splitters ST1 and ST2 arranged in the beam path of light source L and are detected by detectors (trigger detector DT for beam splitter ST1 and detectors $D1_0$ and $D2_1$ for beam splitter ST2) downstream from beam splitters ST1 and ST1 according to the split.

Detectors DT, $D1_0$ and $D2_1$ are connected to detection unit E. A random number is generated only if the photons registered at the individual detectors DT, $D1_0$ and $D2_1$ correspond in their totality to a previously defined photon count scheme which has been input into the computer of the detection unit.

The mathematical principles and the possible embodiments of the method according to the present invention are explained in greater detail below with reference to Figure 1.

Light source L has such a weak light intensity that it emits individual photons or it always emits photon swarms of n photons with a certain probability. These photon swarms are then either resolved in detectors DT, $D1_0$ and $D2_1$ or counted as a whole as a single result. Probability p_n that n photons will arrive at the detector at the same time or will be counted as a single result is described by a Poisson distribution.

$$p_n = \frac{\bar{n}^n}{n!} e^{-\bar{n}} \qquad (1)$$

$\bar{n}$ is the average number of photons at the detector per measurement time. Although the light source has different statistics if it is thermal light (halogen lamp), chaotic

light (spectral line) or laser light, equation (1) applies to all these light sources as long as the coherent time of a thermal or chaotic source is short in comparison with the measurement time of the detector. Equation (1) always applies to laser light. With a simple beam splitter with two detectors, as illustrated by beam splitter ST2 and detectors $D1_0$ and $D2_1$ in Figure 1, the electronics of the counting processes are set up so that a result is only ever counted when only one of detectors $D1_0$ or $D2_1$ responds. If both detectors $D1_0$ and $D2_1$ respond within the measurement time, the counting event is discarded. If a swarm of photons is split on beam splitter ST2, the result is not used. A counting event is used only if the swarm enters detector $D1_0$ completely or enters detector $D2_1$ completely and is counted. With a swarm of n photons, this means that only 2 of n+1 events are counted, and therefore, equation (1) is to be multiplied by $\frac{2}{n+1}$ to describe the probability with which counting events occur with a photon swarm. Therefore, probability p_n that a usable counting event will occur at an average photon count $\bar{n}$ is as follows for the simple beam splitter, corresponding to beam splitter ST2, and one of the light sources L of a low power described above

$$p_n^{(1)} = \frac{\bar{n}^n}{n!} e^{-\bar{n}} \cdot \frac{2}{n+1} \quad \textit{simple beam splitter} \qquad (2)$$

According to the present invention, another beam splitter ST1, preferably a trigger beam splitter, is connected upstream from simple beam splitter ST2 (Figure 1). As in the first case, the electronic counters of both detectors $D1_0$ and $D2_1$ are connected so that a random number is determined only when only one or only the other detector $D1_0$ or $D2_1$ responds. In addition, however, trigger detector DT of beam splitter ST1 must not respond in this case. Transit time effects between trigger detector DT of first beam splitter ST1 and detectors $D1_0$ and $D2_1$ of second beam splitter ST2 are compensated optically or electronically. If there is a swarm of n photons and at least one photon of the swarm reaches trigger detector DT, the event is not counted. An event is counted as (0) or (1) only if no photon goes over first beam splitter ST1 to

trigger detector DT and also if all n photons at second beam splitter ST2 go either completely to detector $D1_0$ or completely to detector $D2_1$. The probability that no photon of the swarm will go to trigger detector DT and the rest will go completely to one of detectors $D1_0$ or $D2_1$ is 4/((n+1)(n+2)), i.e., the probability $p_n^{(2)}$ that a counting event will occur with a swarm of n photons is

$$p_n^{(2)} = \frac{\bar{n}^n}{n!} e^{-\bar{n}} \cdot \frac{4}{(n+1)(n+2)} \quad \begin{matrix} \textit{beam splitter ST2 with} \\ \textit{beam splitter ST1 connected upstream} \end{matrix} \tag{3}$$

Equation (3) applies to the case when beam splitter ST1 has splitting ratio 1/3 : 2/3, but beam splitter ST2 has splitting ratio 1/2 : 1/2. In this case, three detectors DT, $D1_0$ and $D2_1$ are weighted equally. Other splitting ratios are possible, but they alter the probabilities according to equation (3).

The method used here makes it progressively less likely that, with an increasing number n of photons emitted during a predefined measurement time, an n-photon swarm will lead to a counting event and thus to a random number. However, there is an increase in the probability that the ideal case in terms of quantum mechanics will occur, namely generation of a random event by a single photon on the beam splitter. Multi-photon events, which in the limit case of greater than n go into the conventional state, are suppressed. Thus, according to the present invention, weak lasers, chaotic or thermal light sources can be used as random generators.

An arrangement of more than one trigger beam splitter in the beam path between light source L and beam splitter ST2 is also conceivable. The trigger detectors of these additional trigger beam splitters are also connected to detection device E. In such an embodiment, the photons detected during the predefined measurement time are registered in the detection device in accordance with their assignment to the individual trigger beam splitters (including beam splitter ST2) and are likewise compared with a predetermined photon scheme stored in detection device E. In such an embodiment,

photon swarms are suppressed to an even greater extent. Random events are recorded, for example, only when none of the trigger detectors responds.

Another defined or variable photon scheme may also be selected with an embodiment having multiple trigger detectors in the beam path of light source L. For example, the photon scheme may include the fact that the trigger detector of every second trigger beam splitter must respond or that only the trigger detector of the first and seventh trigger beam splitter must respond. In each of these cases, the counting probability for the photon swarm is reduced.

An interesting example is an arrangement according to Figure 1, where the random events at second beam splitter ST2 are counted only when one or more photons is registered by trigger detector DT of beam splitter ST1. In this case, swarms with only <u>one</u> photon are not used at all for random generation. Since detectors today also have some very unpleasant properties, such as a low quantum efficiency and dead times, the trade-in for additional trigger beam splitters is also additional electronic problems and higher costs. Thus, in practice, preferably only one additional trigger beam splitter is used.

List of reference notation

L	light source
ST1	first beam splitter (trigger beam splitter)
ST2	second beam splitter
E	detection device
DT	trigger detector of the first beam splitter
$D1_0$	I
	I detectors of the second beam splitter
$D2_1$	I
n	number of photons emitted by the light source during a defined measurement time

Patent Claims

1. Method of generating binary sequences of random numbers based on the principle of random selection of the path of photons on a beam splitter and generating a random number by using two detectors downstream from a beam splitter, where the counting electronic means of the two detectors are wired so that a random number is generated when only one of the detectors responds, characterized in that the photons/photon swarms emitted during a defined measurement time by a photon source designed as a light source (L) of a low power according to the random principle are split by at least two beam splitters (ST1; ST2) arranged one after the other in the beam path of the light source (L) and are detected by downstream detectors (DT; $D1_0$, $D2_1$) connected to the detection device (E) in accordance with the split by the beam splitters (ST1, ST2), and a random number is generated only if the photons registered at the individual detectors (DT; $D1_0$, $D2_1$) correspond in their totality to a previously defined photon scheme.

2. Method according to Claim 1, characterized in that with two beam splitters (ST1, ST2) arranged one after the other in the beam path of the light source (L), the photon counting scheme on which generation of the random number is based is in turn based on generating a random number only when no photon is registered at the trigger detector (DT) of the first beam splitter (ST1) during the predefined measurement period and at least one photon is registered at only one of the detectors ($D1_0$) or ($D2_1$) downstream from the second beam splitter (ST2).

3. Method according to Claim 1, characterized in that with two beam splitters (ST1, ST2) arranged one after the other in the beam path of the light source, the photon counting scheme on which the generation of the random number is based is in turn based on generating a random number only when at least one photon is registered on the detector (DT) of the first beam splitter (ST1) during the predefined measurement time and at least one photon is registered at only one of the two detectors ($D1_0$) and

($D2_1$) downstream from the second beam splitter (ST2).

4. Method according to Claim 1, characterized in that for the case when more than two trigger beam splitters are arranged in the beam path between the light source (L) and the beam splitter (ST2), the photon scheme is designed mathematically so that a random number is generated only when a photon swarm with a number of photons defined by the predefined photon scheme appears at the detectors of the beam splitter (ST2) and the trigger detectors of the additional trigger beam splitters.

5. Arrangement for generating binary sequences of random numbers, including
- a light source designed as a photon source,
- a beam splitter downstream from the light source and having two detectors downstream from the beam splitter, and
- a detection device downstream from the detectors, including counters and computer, for generating the random numbers,

characterized in that a light source (L) of a low power is used as the photon source from which both individual photons as well as photon swarms can be emitted according to the random principle, and at least one additional beam splitter, preferably a trigger beam splitter (ST1), is arranged in the beam path between the light source (L) and the beam splitter (ST2) arranged in the beam path of the light source (L), the additional beam splitter being connected by a detector, preferably a trigger detector (DT), to the detection device (E).

6. Arrangement according to Claim 5, characterized in that an attenuated laser is used as light source (L).

7. Arrangement according to Claim 5, characterized in that a thermal light source is used as light source (L).

8. Arrangement according to Claim 5, characterized in that an spectral lamp is used as

light source (L).

9. Arrangement according to Claim 5, characterized in that a light emitting diode is used as light source (L).

10. Arrangement according to Claim 4, characterized in that a pinched light source is used as light source (L).

Abstract of the Disclosure

1.1. Method and arrangement for generating binary sequences of random numbers

2.1. The object is to provide a cost-effective method and an arrangement for generating binary sequences of random numbers. The method of achieving this should be such that integration on a chip card is easily possible.

2.2. This method is based on the principle of random selection of the path of photons on a beam splitter and generating a random number by using two detectors ($D1_0$, $D2_1$) downstream from a beam splitter (ST2). To generate photons, a light source (L) of a low power is used, and an additional beam splitter (ST1) is connected upstream from the beam splitter (ST2). The photons emitted by the light source (L) during a predefined measurement time are split by the beam splitters (ST1, ST2) arranged one after the other in the beam path of the light source (L). The random sequence is generated when the splitting of the photons matches a predefined photon scheme.

2.3. This method makes available an inexpensive random generator which can be integrated into a chip card easily in particular because of the light source (L) used.

3.0. Figure 1

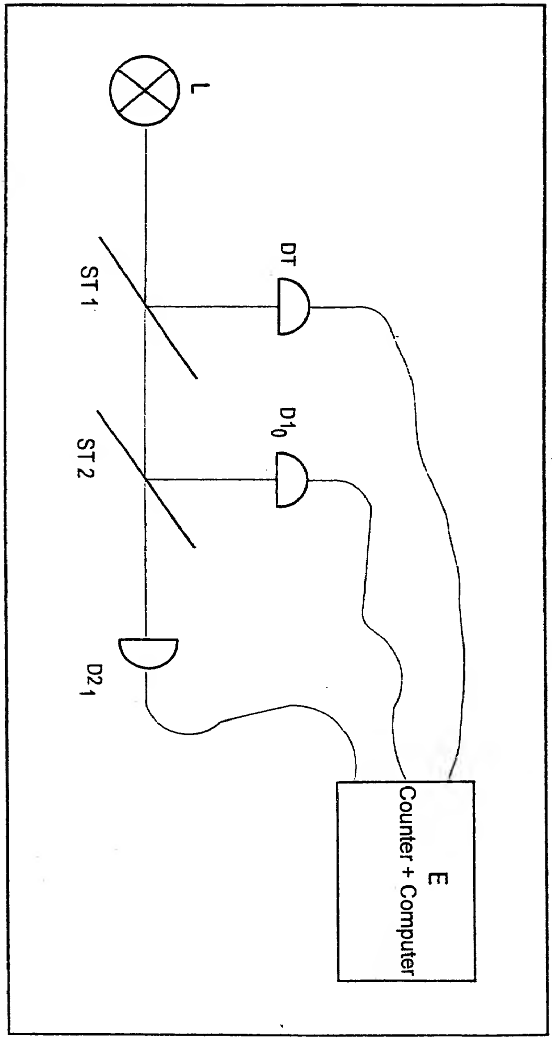

Fig. 1

20 JAN 2000

09/402322

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE

DECLARATION AND POWER OF ATTORNEY	ATTORNEY'S DOCKET NO. 2345/91

As a below named inventor, I hereby declare that:

My residence, post office address, and citizenship are as stated below next to my name,

I believe I am an original, first, and joint inventor of the subject matter that is claimed and for which a patent is sought on the invention entitled **METHOD AND ARRANGEMENT FOR GENERATING BINARY SEQUENCES OF RANDOM NUMBERS**, the specification of which was filed as PCT/EP98/08057 on 10 December 1998.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a).

PRIOR FOREIGN APPLICATION(S)

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

COUNTRY	APPLICATION NUMBER	DATE OF FILING (day, month, year)	DATE OF ISSUE (day, month, year)	PRIORITY CLAIMED UNDER 35 U.S.C. § 119
GERMANY	**198 06 178.1**	**2 February 1998**		**YES**

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorneys:
Richard L. Mayer (Reg. No. 22,490)
Erik R. Swanson (Reg. No. 40,833)

SEND CORRESPONDENCE, AND DIRECT TELEPHONE CALLS TO:

Richard L. Mayer
KENYON & KENYON
One Broadway
New York, New York 10004
(212) 425-7200 (phone)
(212) 425-5288 (facsimile)

EL179105087

I declare that all statements made herein of my own knowledge are true and all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under § 1001 of Title 18 of the United States Code and that such willful statements may jeopardize the validity of the application or any patent issuing thereon.

FULL NAME OF INVENTOR	FAMILY NAME **DULTZ**	FIRST GIVEN NAME **Wolfgang**	SECOND GIVEN NAME
RESIDENCE & CITIZENSHIP	CITY **D-65936 Frankfurt amMain**	STATE OR FOREIGN COUNTRY **Germany**	COUNTRY OF CITIZENSHIP **Germany**
POST OFFICE ADDRESS	POST OFFICE ADDRESS **Marienbergerstr. 37**	CITY **D-65936 Frankfurt amMain**	STATE & ZIP CODE/COUNTRY **Germany**
Signature	W. Dultz	Date	26.9.99
FULL NAME OF INVENTOR	FAMILY NAME **DULTZ**	FIRST GIVEN NAME **Gisela**	SECOND GIVEN NAME
RESIDENCE & CITIZENSHIP	CITY **D-65936 Frankfurt am Main**	STATE OR FOREIGN COUNTRY **Germany**	COUNTRY OF CITIZENSHIP **Germany**
POST OFFICE ADDRESS	POST OFFICE ADDRESS **Marienbergerstr. 37**	CITY **D-65936 Frankfurt amMain**	STATE & ZIP CODE/COUNTRY **Germany**
Signature	Date 26.9.99	G. Dultz	

3W

FULL NAME OF INVENTOR	FAMILY NAME HILDEBRANDT	FIRST GIVEN NAME Eric	SECOND GIVEN NAME
RESIDENCE & CITIZENSHIP	CITY D-60487 Frankfurt amMain	STATE OR FOREIGN COUNTRY Germany	COUNTRY OF CITIZENSHIP Germany
POST OFFICE ADDRESS	POST OFFICE ADDRESS Ginnheimer Str. 20	CITY D-60487 Frankfurt amMain	STATE & ZIP CODE/COUNTRY Germany
Signature		Date 20. 9. 1999	

4W

FULL NAME OF INVENTOR	FAMILY NAME SCHMITZER	FIRST GIVEN NAME Heidrun	SECOND GIVEN NAME
RESIDENCE & CITIZENSHIP	CITY D-93051 Regensburg	STATE OR FOREIGN COUNTRY Germany	COUNTRY OF CITIZENSHIP Germany
POST OFFICE ADDRESS	POST OFFICE ADDRESS Koenig-Philipp-Weg 25	CITY D-93051 Regensburg	STATE & ZIP CODE/COUNTRY Germany
Signature		Date	

737185US
10 Rec'd PCT/PTO 20 JAN 2000
09/402322

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE

DECLARATION AND POWER OF ATTORNEY	ATTORNEY'S DOCKET NO. **2345/91**

As a below named inventor, I hereby declare that:

My residence, post office address, and citizenship are as stated below next to my name,

I believe I am an original, first, and joint inventor of the subject matter that is claimed and for which a patent is sought on the invention entitled **METHOD AND ARRANGEMENT FOR GENERATING BINARY SEQUENCES OF RANDOM NUMBERS**, the specification of which was filed as PCT/EP98/08057 on 10 December 1998.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a).

PRIOR FOREIGN APPLICATION(S)

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

COUNTRY	APPLICATION NUMBER	DATE OF FILING (day, month, year)	DATE OF ISSUE (day, month, year)	PRIORITY CLAIMED UNDER 35 U.S.C. § 119
GERMANY	**198 06 178.1**	**2 February 1998**		**YES**

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorneys:
Richard L. Mayer (Reg. No. 22,490)
Erik R. Swanson (Reg. No. 40,833)

SEND CORRESPONDENCE, AND DIRECT TELEPHONE CALLS TO:

Richard L. Mayer
KENYON & KENYON
One Broadway
New York, New York 10004
(212) 425-7200 (phone)
(212) 425-5288 (facsimile)

I declare that all statements made herein of my own knowledge are true and all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under § 1001 of Title 18 of the United States Code and that such willful statements may jeopardize the validity of the application or any patent issuing thereon.

FULL NAME OF INVENTOR	FAMILY NAME **DULTZ**	FIRST GIVEN NAME **Wolfgang**	SECOND GIVEN NAME
RESIDENCE & CITIZENSHIP	CITY **D-65936 Frankfurt amMain**	STATE OR FOREIGN COUNTRY **Germany**	COUNTRY OF CITIZENSHIP **Germany**
POST OFFICE ADDRESS	POST OFFICE ADDRESS **Marienbergerstr. 37**	CITY **D-65936 Frankfurt amMain**	STATE & ZIP CODE/COUNTRY **Germany**
Signature		Date	

FULL NAME OF INVENTOR	FAMILY NAME **DULTZ**	FIRST GIVEN NAME **Gisela**	SECOND GIVEN NAME
RESIDENCE & CITIZENSHIP	CITY **D-65936 Frankfurt am Main**	STATE OR FOREIGN COUNTRY **Germany**	COUNTRY OF CITIZENSHIP **Germany**
POST OFFICE ADDRESS	POST OFFICE ADDRESS **Marienbergerstr. 37**	CITY **D-65936 Frankfurt amMain**	STATE & ZIP CODE/COUNTRY **Germany**
Signature	Date		

FULL NAME OF INVENTOR	FAMILY NAME **HILDEBRANDT**	FIRST GIVEN NAME **Eric**	SECOND GIVEN NAME
RESIDENCE & CITIZENSHIP	CITY **D-60487 Frankfurt amMain**	STATE OR FOREIGN COUNTRY **Germany**	COUNTRY OF CITIZENSHIP **Germany**
POST OFFICE ADDRESS	POST OFFICE ADDRESS **Ginnheimer Str. 20**	CITY **D-60487 Frankfurt amMain**	STATE & ZIP CODE/COUNTRY **Germany**
Signature		Date	

FULL NAME OF INVENTOR	FAMILY NAME **SCHMITZER**	FIRST GIVEN NAME **Heidrun**	SECOND GIVEN NAME
RESIDENCE & CITIZENSHIP	CITY **D-93051 Regensburg**	STATE OR FOREIGN COUNTRY **Germany**	COUNTRY OF CITIZENSHIP **Germany**
POST OFFICE ADDRESS	POST OFFICE ADDRESS **Koenig-Philipp-Weg 25**	CITY **D-93051 Regensburg**	STATE & ZIP CODE/COUNTRY **Germany**
Signature	Heidrun Schmitzer	Date	1. Okt. 99